(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 05007202 A

(43) Date of publication of application: 14.01.93

(51) Int. Cl H04L 9/28
H04K 1/04

(21) Application number: 03288717

(22) Date of filing: 05.11.91

(30) Priority: 05.11.90 JP 02299492

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

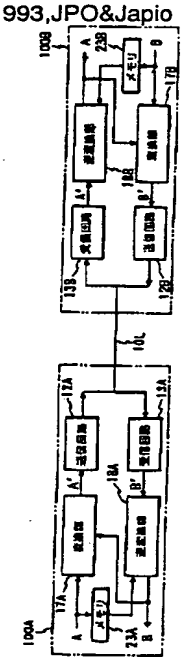
(72) Inventor: OKADA KENJI
MANO FUMIO
TOKURA NOBUYUKI
KUMOSAKI KIYOMI
MIKI NORIMOTO

(54) ENCIPHERING COMMUNICATION EQUIPMENT AND ENCIPHERING TRANSMISSION SYSTEM

(57) Abstract:

PURPOSE: To realize an enciphering communication device and an enciphering transmission system with high secret.

CONSTITUTION: In an enciphering transmission system where a first communication equipment 100A and a second communication equipment 100B are connected by a transmission line 10L, a first communication equipment 100A has a converting part 17A to encipher an information signal A to be transmitted with a signal corresponding to a receiving signal, and a second communication equipment 100B has an information memory 23B to store information B to be transmitted to the first communication equipment 100A as key information and a reverse converting part 18B to decode an enciphering signal A' received from the first communication equipment 100A with the key information read from the information memory 23B. An enciphering communication equipment 100A has the converting part 17A to encipher a transmitting information signal A with the signal corresponding to the receiving signal, an information memory 23A to store the information signal A to be transmitted as the key information and a reverse converting part 18A to decode a receiving signal B' with the key information from the information memory 23A. As the transmitting information signal is changed, the key information is changed and the secret is increased.



A-99EC0275

P-662

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－7202

(43)公開日　平成５年(1993)１月14日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/28					
Ｈ０４Ｋ　1/04		7117－5Ｋ			
		7117－5Ｋ	Ｈ０４Ｌ　9/ 02	Ａ	

審査請求　未請求　請求項の数６（全 19 頁）

(21)出願番号　特願平3－288717

(22)出願日　平成３年(1991)11月５日

(31)優先権主張番号　特願平2－299492

(32)優先日　平２(1990)11月５日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　岡田　實治
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　真野　文雄
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　戸倉　信之
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

最終頁に続く

(54)【発明の名称】　暗号化通信装置及び暗号化伝送システム

(57)【要約】

【目的】　秘話性の高い暗号化通信装置及び暗号化伝送システムを実現する。

【構成】　第１通信装置１００Ａと第２通信装置１００Ｂとが伝送路１０Ｌにより接続された暗号化伝送システムにおいて、第１通信装置１００Ａは受信信号に対応した信号を使って送信すべき情報信号Ａを暗号化する変換部１７Ａを有し、第２通信装置１００Ｂは第１通信装置１００Ａに送信すべき情報Ｂをキー情報として記憶する情報メモリ２３Ｂと、情報メモリ２３Ｂから読出したキー情報を使って第１通信装置１００Ａから受信した暗号化信号Ａ´を復号する逆変換部１８Ｂを有している。暗号化通信装置１００Ａは受信信号に対応した信号を使って送信情報信号Ａを暗号化する変換部１７Ａと、送信すべき情報信号Ａをキー情報として記憶する情報メモリ２３Ａと、情報メモリ２３Ａからのキー情報を使って受信信号Ｂ´を復号する逆変換部１８Ａを有している。送信情報信号が変化するにつれキー情報が変化し秘話性の高い暗号化伝送システム及び暗号化通信装置が実現できる。

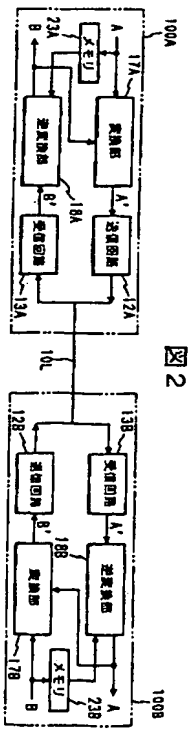


図２

【特許請求の範囲】

【請求項１】　少なくとも第１と第２の通信装置が伝送媒体を介して接続された暗号化伝送システムにおいて、上記第１通信装置は上記伝送媒体を通して供給された上記第２通信装置からの信号を受信する第１受信手段と、上記第１受信手段から出力される上記第２通信装置からの受信信号に対応した信号を使って上記第２通信装置へ送信すべき情報信号を暗号化して暗号化信号を生成する変換手段と、上記暗号化信号を上記伝送媒体に送出する第１送信手段とを含み、上記第２通信装置は上記第１通信装置に送信すべき情報信号に対応した信号をキー情報として記憶するための情報記憶手段と、上記送信信号を上記伝送媒体に送出する第２送信手段と、上記伝送媒体を通して供給された上記第１通信装置からの上記暗号化信号を受信する第２受信手段と、上記情報記憶手段からの前回送信した上記情報信号に対応する上記キー情報を使って上記第２受信手段で受信された上記暗号化信号を復号して復号化情報信号を出力する逆変換手段とを含む暗号化伝送システム。

【請求項２】　請求項１記載の暗号化伝送システムにおいて、上記第１通信装置の上記変換手段は上記第２通信装置からの受信信号が入力情報として与えられ、それに対応したランダムパタンを生成する第１ランダムパタン生成手段と、上記生成されたランダムパタンと送信すべき上記情報信号との論理演算を行って上記暗号化信号を生成する第１論理演算手段とを含み、上記第２通信装置の上記逆変換手段は上記情報記憶手段からの上記キー情報が入力情報として与えられ、それに対応したランダムパタンを生成する上記第１ランダムパタン生成手段と同じ構成の第２ランダムパタン生成手段と、上記第２ランダムパタン生成手段により生成された上記ランダムパタンと受信された上記暗号化信号とを論理演算を行って上記暗号化信号を復号する第２論理演算手段とを含む。

【請求項３】　請求項１に記載の暗号化伝送システムにおいて、上記第２通信装置と同じ構成の第３通信装置が設けられ、上記伝送媒体は光ファイバ伝送路であり、上記第２及び第３通信装置は方向性光分岐手段により上記光ファイバ伝送路に接続されており、上記第１通信装置内の上記変換手段は上記第２及び第３通信装置に送信すべき送信情報信号をそれぞれ上記第２及び第３通信装置から受信した受信信号を使って暗号化する第１及び第２変換部を含み、上記第１送信手段は上記第１及び第２変換部からの暗号化信号を多重化する多重化手段と、その多重化信号を上記光ファイバ伝送路に送出する光送信回路を含み、上記第１受信手段は上記光ファイバ伝送路から与えられた多重化信号を受信する第１光受信回路と、上記第１光受信回路からの受信多重化信号を上記第２及び第３通信装置からの受信信号に分離する多重分離手段を含み、各上記第２及び第３通信装置内の上記第２受信手段は上記方向性光分岐手段から多重化信号を受信する第２光受信回路と、上記受信した多重化信号から自分に宛てられた受信信号を分離する分離回路とを含む。

【請求項４】　請求項１記載の暗号化伝送システムにおいて、上記第２通信装置と同じ構成の第３通信装置が設けられ、上記伝送媒体を通じて上記第１通信装置に接続されており、上記第１通信装置の上記第１受信手段は上記伝送媒体を通して上記第２及び第３通信装置から送出され、互いに多重化された多重化信号を受信する第１受信回路と、上記受信多重化信号を上記第２及び第３通信装置からの受信信号に分離する多重分離手段と、上記第２及び第３通信装置へ送信すべき情報信号に対応した信号をキー情報として記憶する第１及び第２情報メモリと、上記多重分離された受信信号をそれぞれ対応した上記第１及び第２情報メモリからの上記キー情報を使って復号化することにより復号化情報信号を出力する第１及び第２逆変換部とを含み、上記第１通信装置の上記変換手段は上記第２及び第３通信装置へ送信すべき情報信号を上記第１及び第２逆変換部からの上記復号化情報信号を使ってそれぞれ暗号化することによりそれぞれ暗号化情報信号を出力する第１及び第２変換部を含み、上記第１送信手段は上記第１及び第２変換部からの上記暗号化情報信号を多重化する多重化手段と、上記多重化された信号を上記伝送媒体に送出する第１送信回路とを含み、上記第２及び第３通信装置のそれぞれにおいて、上記第２受信手段は上記伝送媒体が供給された多重化信号を受信する第２受信回路と、上記第２受信回路からの受信多重化信号から自分に宛てられた受信信号を分離して上記逆変換手段に与える分離回路とを含み、上記第２送信手段は上記逆変換手段からの上記復号化情報信号に対応した信号を使って上記第１通信装置へ送信すべき情報信号を暗号化する変換部と、その暗号化情報信号を上記伝送媒体に送出する第２送信回路を含む。

【請求項５】　伝送媒体を通して供給された信号を受信する受信手段と、上記受信手段からの受信信号に対応した信号の少なくとも一部を使って送信情報信号を論理変換することにより暗号化信号を生成する変換手段と、上記暗号化信号を上記伝送媒体に送出する送信手段と、上記送信情報信号に対応した信号をキー情報として記憶するための情報記憶手段と、上記情報記憶手段からの上記キー情報を使って上記受信手段からの上記受信信号を論理逆変換することにより上記受信信号を復号して復号化情報信号を出力する逆変換手段、とを含む暗号化通信装置。

【請求項６】　請求項５に記載の暗号化通信装置において、上記変換手段は上記受信信号に対応した信号の少なくとも一部を使ってランダムパタンを生成する第１ランダムパタン生成手段と、上記第１ランダムパタン生成手段からのランダムパタンと上記送信情報信号を論理演算して上記暗号化信号を出力する第１論理演算手段を含み、上記逆変換手段は上記情報記憶手段からの上記キー

情報の少なくとも一部を使ってランダムパタンを生成する上記第２ランダムパタン生成手段と、上記第２ランダムパタン生成手段からのランダムパタンと上記受信信号を論理逆変換演算して上記復号化情報信号を出力する第２論理演算手段とを含む。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は複数の暗号化通信装置が伝送路を介して互いに秘話通信を行う暗号化伝送システム及び暗号化通信装置に関する。

【０００２】

【従来の技術】従来の秘話通信を行う伝送システムにおいては例えば図１に示すように伝送路１０Ｌに接続された暗号化通信装置１００Ａと１００Ｂがそれぞれ送信すべき情報を暗号化して相手に送信し、また相手からの暗号化受信信号を解読して情報を得る。各暗号化通信装置はその１つ１００Ａで説明すると、送信すべき情報信号Ａはスクランブル回路１１Ａにより暗号化され、送信回路１２Ａにより伝送路１０Ｌに送出される。スクランブル回路１１Ａは情報信号Ａを擬似ランダムパタン発生器１５Ａにより発生される固定のランダムパターンＫ１（暗号化キー）で暗号化する。暗号化された信号Ａ′は送信回路１２Ａにより伝送路１０Ｌを通して通信装置１００Ｂに送出される。一方通信装置１００Ｂから伝送路１０Ｌを通して受信回路１３Ａにより受信された信号Ｂ′はデスクランブル回路１４Ａにおいて擬似ランダムパタン発生器１６Ａにより発生された固定のランダムパターンＫ２（解読キー）を使って解読され、通信装置１００Ｂからの情報信号Ｂが得られる。

【０００３】

【発明が解決しようとする課題】図１のような従来の暗号化伝送システムにおいては、秘話性を高かめるため暗号化のために使用するランダムパターンＫ１，Ｋ２として非常に長いランダムパターンを使用し、かつ複雑な変換を行おうとすると、スクランブル回路１１Ａ，１１Ｂ，及びデスクランブル回路１４Ａ，１４Ｂの回路規模が大きくなり、価格が高くなる欠点がある。しかも使用するランダムパターンＫ１，Ｋ２は固定されているため、第３者に解読される可能性を皆無に近かづけることは困難である。例えば同様の構成の暗号化通信装置が１００Ａ，１００Ｂ以外にも伝送路１０Ｌに接続されている場合に、それぞれの通信装置のスクランブル回路及びデスクランブル回路を同様な仕様の回路で構成し、同様の変換規則や変換周期を適用すると通信装置間の秘話性を低くめてしまう。

【０００４】この発明の目的は構成が簡単でかつ秘話性の高い暗号化通信装置を提供することである。この発明のもう１つの目的は構成が簡単でかつ秘話性の高い暗号化伝送システムを提供することである。

【０００５】

【課題を解決するための手段】この発明による暗号化通信装置は受信された信号を用いて送信信号を論理変換し、それによって暗号化信号を生成する変換手段と、その暗号化信号を伝送路に送出する送信回路手段と、上記送信信号に対応した信号をキー情報として記憶する情報記憶手段と、上記伝送路から与えられる暗号化信号を受信する受信回路手段と、上記情報記憶手段からの上記キー情報を使って上記受信暗号化信号を論理逆変換することにより解読した受信信号を出力する逆変換手段とを含む。

【０００６】この発明による暗号化伝送システムは少なくとも第１と第２の通信装置が伝送路を介して接続され、上記第１通信装置は上記第２通信装置からの信号を受信する第１受信回路手段と、その受信信号を使って送信信号を論理変換し、それによって暗号化信号を生成する変換手段と、その暗号化信号を上記伝送路に送出する第１送信回路手段とを含み、上記第２通信装置は送信すべき信号をキー情報として記憶する情報記憶手段と、上記送信すべき信号を上記伝送路に送出する第２送信回路手段と、上記伝送路から与えられる暗号化信号を受信する第２受信回路手段と、上記情報記憶手段からの上記キー情報を使って上記受信した暗号化信号を論理逆変換することにより解読した信号を出力する逆変換手段とを含む。

【０００７】

【作用】この発明の暗号化通信装置及び暗号化伝送システムによれば通信相手からの順次変化する受信信号を使って送信信号を暗号化しているので、通信相手以外の者が暗号化された送信信号を解読することは非常に困難である。また受信信号を使った送信信号の暗号化は比較的簡単な論理変換によっても高い秘話性を実現することが可能である。従って各通信装置の回路規模を比較的に小さく、安価に製造することができる。

【０００８】図２はこの発明を適用した２つの暗号化通信装置１００Ａ，１００Ｂが伝送路１０Ｌに接続された暗号化伝送システムの実施例を示している。伝送路１０Ｌに接続される暗号化通信装置は２つ以上でもよく、それぞれ同様の構成とされているので代表して通信装置１００Ａを以下に説明する。暗号化通信装置１００Ａは送信回路１２Ａと、受信回路１３Ａと、変換部１７Ａと逆変換部１８Ａと、送信情報メモリ２３Ａとによって構成されている。変換部１７Ａは受信情報信号Ｂと送信情報信号Ａとの排他的論理和をとる排他的論理和回路や、その他の論理演算回路のような簡単なものでよく、逆変換部１８Ａも同様である。あらかじめ決めた長さの送信すべき情報信号Ａは変換部１７Ａに与えられ、逆変換部１８Ａからの最新の復号情報信号Ｂを使って論理変換により暗号化されると共にキー情報として情報メモリ２３Ａに与えられ、次の受信暗号化情報信号Ｂ′の復号化まで記憶される。暗号化された信号Ａ′は送信回路１２Ａに

より伝送路１０Ｌを通して相手暗号化通信装置１００Ｂに送出される。

【０００９】その後伝送路１０Ｌを通して相手暗号化装置１００Ｂから受信回路１３Ａに供給された受信暗号化信号Ｂ′は逆変換部１８Ａにおいて情報メモリ２３Ａから読出したキー情報信号Ａを使って論理逆変換により解読（復号）され、情報信号Ｂが得られる。一方、次に送信すべき情報信号Ａが新しいキー情報として情報メモリ２３Ａに与えられて内容が書き換えられ、またその情報信号Ａが変換部１７Ａに与えられる。復号された情報信号Ｂはこの送信すべき情報信号Ａの暗号化のために変換部１７Ａに与えられる。このようにして情報信号Ｂを使って暗号化された信号Ａ′は暗号化通信装置１００Ｂにおいて情報メモリ２３Ｂに記憶してあるキー情報信号Ｂを使って復号することが可能であり、また暗号化通信装置１００Ｂにおいて復号された情報信号Ａを使って暗号化された信号Ｂ′は暗号化通信装置１００Ａにおいて情報メモリ２３Ａに記憶してある情報信号Ａを使って復号することが可能である。しかしながら情報信号Ａ，Ｂは随時変化していくので情報信号Ａ及びＢのいずれも得ていない通信装置においては暗号化信号Ａ′及びＢ′を解読することは困難である。

【００１０】図２の実施例の動作例を図３の表Ｉを参照して説明する。ただし簡単のため各情報信号Ａ，Ｂは８ビット長であり、変換部１７Ａ，１７Ｂ及び変換部１８Ａ，１８Ｂはすべて排他的論理和回路で構成するものとする。また初期状態として情報メモリ２３Ａ，２３Ｂの内容はすべて“０”であり、逆変換部１８Ａの出力Ｂの初期値B_0はオール“０”であるとする。暗号化通信装置１００Ａは情報信号A_1，A_2，…を順次送信するものとし、暗号化通信装置１００Ｂは情報信号Ｂ$_1$，B_2，…を順次送信するものとする。更に、図３中に使用されている排他的論理和を表す一般的な記号である丸十字は以下の説明文において記号＊で表す。

【００１１】まず暗号化通信装置１００Ａにおいては情報信号A_1：１０１０１０１０をキー情報としてメモリ２３Ａに格納すると共に変換部１７Ａに与え受信情報信号初期値B_0：００００００００との排他的論理和A_1＊B_0＝A_1′を１ビットずつ演算し、その結果A_1′：１０１０１０１０を相手通信装置１００Ｂに送信する。通信装置１００Ｂでは逆変換部１８Ｂによりメモリ２３Ｂ内のキー情報の初期値B_0：００００００００と受信信号A_1′との排他的論理和A_1′＊B_0＝A_1を１ビットずつ演算して受信情報信号A_1：１０１０１０１０を得る。更に送信すべき情報信号B_1：００００１１１１を新しいキー情報としてメモリ２３Ｂに書込むと共に変換部１７Ｂにより受信情報信号A_1との排他的論理和A_1＊B_1＝B_1′を１ビットずつ演算し、その結果Ｂ′$_1$＝１０１００１０１を送信する。通信装置１００Ａは受信信号B_1′とメモリ２３Ａの内容A_1との排他的論理和A_1＊B_1′＝B_1を逆変換部１８Ａで演算してB_1＝００００１１１１を得る。更に次に送信すべき情報信号A_2：００１１００１１でメモリ２３Ａを書き換えると共に変換部１７ＡでA_2＊B_1＝A_2′を演算し、その結果A_2′＝００１１１１００を送信する。通信装置１００Ｂにおいてはメモリ２３Ｂの内容B_1と受信信号A_2′とから、A_2′＊B_1＝A_2を逆変換部１８Ｂで演算して情報信号A_2＝００１１００１１を得る。更に次に送信すべき情報B_2＝１１１０００１０でメモリ２３Ｂを書き換えると共に変換部１７ＢによりA_2＊B_2＝B_2′を演算してその結果B_2′＝１１０１０００１を送信する。通信装置１００Ａではメモリ２３Ａの容内A_2と受信信号B_2′からA_2＊B_2′＝B_2を逆変換部１８Ａにより演算し、以下同様な手順が繰り返される。

【００１２】ところで上述の例のように変換部１７Ａを簡純な排他的論理和回路のみで構成した場合、図３を参照して説明したように通信の開始時に受信情報信号Ｂの初期値B_0がオール“０”であると、最初の送信情報信号A_1は排他的論理和回路による変換後も同じ信号即ちA_1′＝A_1となってしまい第３者に対し、解読のための手掛かりを与えてしまう。同様に通信中においての送信情報信号Ａがたまたまオール“０”となるとその時受信した情報信号Ｂがそのまま変換部１７Ａから出力されてしまい第３者に対し解読の手掛りを与えてしまう。

【００１３】情報信号Ａ及び／又はＢがオール“１”の場合も同様である。このような生の情報の流出を避けるには第１図と同様に第４図に示すように送信情報信号Ａをスクランブル回路１１Ａにおいて擬似ランダムパタン発生器１５Ａからの固定ランダムパタンＫ１により論理変換してから図２におけると同様の送信処理を行い、逆変換部１８Ａから出力された受信情報信号はデスクランブル回路１４Ａにおいて擬似ランダムパタン発生器１６Ａからの固定ランダムパタンＫ２により論理逆変換すればよい。スクランブル回路１１Ａ及びデスクランブル回路１４Ａとしては例えば排他的論理和回路や他の論理演算回路を使用することができる。

【００１４】なお、スクランブル回路１１Ａは本来送信情報信号Ａをランダム化（交流化）するためのものであり、それ自体は暗号化を目的とするものではない。従って、キー情報の初期値をオール“０”及びオール“１”以外のあらかじめ決めた値に設定し、しかも送信情報信号Ａが“０”の連続または“１”の連続とならない保証があれば、スクランブル処理を行わないでもよい。逆に、スクランブル処理を行うことにより秘話性を高めることが可能となる。更に通信装置１００Ａと相手通信装置（図示せず）とが使用するスクランブルパタン（擬似ランダムパタン）Ｋ１とＫ２が同じ長さでも異なるパタンとなるように選べばそれだけ秘話性は高くなり、更に長さ（ビット数）を異ならせれば一層秘話性が向上す

る。また上述の例では例えば暗号化通信装置１００Ａのスクランブル回路１１Ａにおける情報信号Ａに対する擬似ランダムパタンＫ１の位相と暗号化通信装置１００Ｂのデスクランブル回路１４Ａにおける受信暗号化信号Ａ’に対する擬似ランダムパタンＫ１の位相を同期させる、いわゆる外部同期方式を用いる必要があるが、このような外部からの固定の擬似ランダムパタンを与えないで、ビット毎に入力される情報信号を例えば排他的論理和回路の一方の入力端子に供給し、その排他的論理和回路の出力をあらかじめ決められた段数のシフトレジスタを通して排他的論理和回路の他方の入力端子に帰還し、排他的論理和回路の出力をスクランブル回路の出力とするような公知の自己同期形スクランブル回路を使用してもよい。このような自己同期形スクランブル回路に対する自己同期形デスクランブル回路もよく知られている。

【００１５】図２及び図４の実施例において更に秘話性を高めるため変換部１７Ａをランダムパタン生成回路と論理変換回路により構成してもよい。その場合の暗号化通信装置１００Ａの例を図５に示す。変換部１７Ａのランダムパタン生成回路２１Ａは復号情報信号Ｂの全ビットまたはそのあらかじめ決めた複数のビットに対応したランダムパタンを生成出力する。論理変換回路２２Ａは前述のような排他的論理和回路やその他の論理演算回路でよい。逆変換部１８Ａも同様にランダムパタン生成回路２４Ａと論理逆変換回路２５Ａにより構成してもよい。このように復号情報信号Ｂにより直接送信情報信号Ａを変換することを避けることにより、例えば通信の開始時や通信中において情報信号Ａ及び／又はＢがたまたまオール“０”またはオール“１”となっても高い秘話性を維持することが可能である。しかも情報信号Ａ、Ｂは順次変化していくので、生成されるランダムパタンも順次変化し、高い秘話性を実現できる。

【００１６】逆変換部１８Ａのランダムパタン生成回路２４Ａは変換部１７Ａのランダムパタン生成回路２１Ａと全く同じ構成である必要はない。暗号化通信装置１００Ｂについても同様であるが変換部１７Ｂと逆変換部１８Ｂのランダムパタン生成回路（図示せず）はそれぞれ暗号化通信装置１００Ａにおける逆変換部１８Ａと変換部１７Ａのランダムパタン生成回路２４Ａ及び２１Ａと全く同じ構成である必要がある。

【００１７】図６は図５におけるランダムパタン生成回路２１Ａ，２４Ａ（変換部１７Ｂ、逆変換部１８Ｂに用いられる場合も同様）の一実施例を示し、割算回路３１と非線形演算回路３２により構成されている。割算回路３１は与えられた情報信号ＡまたはＢ、またはその一部をあらかじめ決めた生成多項式で割算し、その剰余を非線型演算回路３２に与える（例えばW. W. Petersonand E. J. Weldon "Errorcorrecting codes, " M. I. T. Press, 1972）。非線型演算回路３２はその出力から入力を推定することが困難な非可逆的演算を行う回路であり、その演算結果はランダムパタンとして出力される。このような非線形演算回路３２を２次のリカーシブフィルタで構成した例を図７に示す。

【００１８】この非線形演算回路３２は演算回路３１から与えられた剰余に対応した初期値が設定され、その初期値からランダムパタンを発生するものであり、図７に示すように例えば２段の並列８ビットシフトレジスタ（即ち２段の遅延回路）を構成する８ビットＤ形フリップフロップ回路４１，４２と、ビットシフタ４３と、８ビット加算器４４とから構成される。各８ビットＤ形フリップフロップ回路４１，４２にそれぞれ設定する８ビットの初期値としては割算回路３１から与えられた剰余のあらかじめ決めた８ビットの同じデータを用いてもよいが、図７の実施例ではその８ビットデータをフリップフロップ回路４１に設定すると共に、論理反転回路５４で前記８ビットデータの全８ビットの論理を反転してフリップフロップ回路４２に設定する。

【００１９】フリップフロップ回路４１に設定された８ビットデータはビットシフタ４３で全ビットが例えば下位方向に所定ビット数、例えば１ビットシフトされ（即ち８ビットデータが２で割算され）、アンダーフローが捨てられると共にその８ビット出力が８ビット加算器４４の一方の入力に与えられる。加算器４４の他方の入力にはフリップフロップ回路４２の８ビットの内容が与えられる。加算により生じたオーバフローは捨てられ、８ビットの加算結果がランダムパタンシーケンス中の部分パタンとして出力されると共にフリップフロップ回路４１のデータ端子Ｄ（８ビット）に与えられている。この状態でフリップフロップ回路４１，４２のクロック端子ＣＫにクロック信号ＣＫが与えられると、フリップフロップ回路４１の８ビットＱ出力がフリップフロップ回路４２に取り込まれると共に、フリップフロップ回路４１に、そのデータ端子Ｄに与えられていたデータが取り込まれ、その結果次の部分パタン（８ビット）が加算器４４から出力される。

【００２０】クロック信号ＣＫは情報信号ＡまたはＢの８ビット毎にフリップフロップ回路４１，４２に与えられ、例えば情報信号Ａ，Ｂの長さが１２８バイトであればクロック信号ＣＫを１２８回与えてからフリップフロップ回路４１，４２をリセット信号Ｒによりリセットし、次の情報信号Ａ，Ｂにもとづいて新しい初期値を再びフリップフロップ回路４１，４２にプリセットし、同様の動作を繰り返す。なお、ビットシフタ４３は入力８ビットデータを上位方向に所定ビット数シフト（即ち２の巾乗の乗算）して、オーバフローを捨ててもよい。このように加算器４４のオーバフローや割算器（または乗算器）４３のアンダフロー（またはオーバフロー）を捨てることにより演算の非可逆性を実現することができる。

【００２１】このように簡単な割算回路３１と２次のリ

カーシブフィルタ３２により構成された図６のランダムパタン生成回路２１Ａにより、入力情報信号Ａ，Ｂに従って一義的に定まるランダムパタンを部分パタン毎に順次生成することができ、かつこれら一連の部分パタンから情報信号Ａ，Ｂを推定することは非常に困難である。リカーシブフィルタ３２の次数を高くすれば更に秘話性を高めることができることは明らかである。

【００２２】図８はランダムパタン生成回路２１Ａ，２４Ａ（通信装置１００Ｂにも同様に設けられる）の更に他の実施例を示し、論理演算回路３３と、識別番号メモリ３４と、デコーダ３５と、固定パタンメモリ３６と、切替スイッチ３７とにより構成されている。識別番号メモリ３４には、その暗号化通信装置にあらかじめ割り当てられた識別番号ＩＤが記憶されている。論理演算回路３３は与えられた情報信号Ａ（またはＢ）と識別番号メモリ３４からの識別番号ＩＤまたはそのあらかじめ決めた一部とを論理演算してその結果をランダムパタンとして切替スイッチ３７を介して出力する。デコーダ３５は入力情報信号Ａ（またはＢ）がオール“０”及びオール“１”であることを検出すると制御信号を出力して切替スイッチ３７を固定パタンメモリ３６側に接続し、固定パタンメモリ３６に保持してあるオール“０”及びオール“１”以外のあらかじめ決めた１つの固定パタンを出力する。このように構成することによりランダムパタン生成回路２１Ａ，２４Ａに与えられる情報信号Ａ（またはＢ）がオール“０”またはオール“１”の場合に識別番号メモリ３４に保持している装置識別番号がそのまま変換回路２２Ａ、または逆変換回路２５Ａに与えられることを防ぐことができる。なお、切替スイッチ３７は論理演算回路３３の出力側ではなく、論理変換回路２２Ａ（論理逆変換回路２５Ａ）の出力側に挿入してもよい。

【００２３】図９はランダムパタン生成回路２１Ａ，２４Ａの更に他の実施例を示す。この実施例は複数、例えば８個の異なるランダムパタンから入力情報信号Ａ（またはＢ）に応じてそのうちの１つを選択して出力するものであり、以下のように構成される。タイマ回路５１は受信回路１３Ａで再生したクロック信号ＣＫとフレーム同期信号ＦＳＹＮが与えられ、後者によりリセットされ、前者を計数し、計数値が所定値に達するとタイムアップ信号ＴＵを出力し、セレクタ５３のロード端子Ｌに与える。フレーム同期信号ＦＳＹＮはタイマ回路５１を通して８進カウンタのリセット端子Ｒにも与えられる。８進カウンタ５２は情報信号Ａ（またはＢ）が与えられ、その一連のビット中の“１”（または“０”）を順次計数する。タイマ回路５１がタイムアップ信号ＴＵをセレクタ５３のロード端子Ｌに与えると、セレクタ５３はその時の８進カウンタ５２の計数値を取り込み、その計数値に従ってランダムパタン発生器Ｒ１～Ｒ８の１つを選択し、そこから発生されるランダムパタンを出力する。各ランダムパタン発生器Ｒ１～Ｒ８としては、例えばシフトレジスタと排他的論理和回路により構成された周知の擬似ランダムパタン発生回路でもよいし、必要な数（ここでは８個）のランダムパタンを記憶したＲＯＭでもよいし、あるいはランダムパタン発生手順をプログラム化したソフトであってもよい。

【００２４】以上いくつかの例で説明したランダムパタン生成回路を用いた暗号化通信装置において、生成したランダムパタンからの入力情報信号の解読を更に困難にするように構成した暗号化通信装置１００Ａの実施例を図１０に示す。図２における暗号化通信装置１００Ａとの相異点は変換部１７Ａ及び逆変換部１８Ａにおいてランダムパタン生成回路２１Ａ及び２４Ａの入力側にパタン縮退回路２６Ａ及び２７Ａをそれぞれ挿入した点である。パタン縮退回路２６Ａ，２７Ａは2^n個の可能な異なる入力パタン（ｎビット）のそれぞれに対し2^nより少ないＭ個の異なるパタンのあらかじめ決めたいずれか１つを割り当てて出力するものであり、従って複数の異なる入力パタンに対し同一の出力パタンが出力される。例えば異なる２つの決められたパタンの受信情報信号Ｂに対しパタン縮退回路２６Ａが同一のパタンを出力すると、ランダムパタン生成回路２１Ａも同一のランダムパタンを出力する。ランダムパタン生成回路２１Ａから出力されたそのランダムパタンから受信情報信号Ｂが前記２つのパタンのいずれであったか判定することはできない。なお図１０の実施例においてランダムパタン生成回路２１Ａとパタン縮退回路２６Ａの位置を入れ替えてもよく、ランダムパタン生成回路２４Ａとパタン縮退回路２７Ａの位置を入れ替えてもよい。

【００２５】図１１は図１０の実施例におけるパタン縮退回路２６Ａ，２７Ａの一実施例を示す。このパタン縮退回路は２段シフトレジスタ４６と、ＡＮＤ回路４７と２段のシフトレジスタ４８とから構成されている。情報信号ＡまたはＢの２ビットが、シフトレジスタ４６にシリアルにロードされる毎にシフトレジスタ４６の２つの段の出力Ｑ１，Ｑ２が入力端子Ｘ１，Ｘ２を介してＡＮＤ回路４７の入力端子に与えられ、それらの論理積が出力端子Ｙ１に出力される。一方出力Ｑ２は入力端子Ｘ２を介して出力端子Ｙ２に出力される。これら出力端子Ｙ１，Ｙ２からの出力はシフトレジスタ４８の２つの段に並列入力され、その後シフトレジスタ４７からシリアルに出力されると共に情報信号Ａ（またはＢ）の次の２ビットがシリアルにシフトレジスタ４５に入力され同様の動作が繰り返される。この結果、端子Ｘ１，Ｘ２に与えられる２ビットパタンと出力端子Ｙ１，Ｙ２に得られる２ビットパタンの関係は図１２の表IIに示すようになる。即ち入力ビットパタンが“００”及び“１０”の場合、いずれも出力ビットパタンは“００”となる。従ってこのパタン縮退回路の出力パタンから入力パタンを推定できる確率はそれだけ低くなる。

【００２６】図１３は図２の実施例における各暗号化通

信装置の他の実施例を通信装置１００Ａで代表して示す。この実施例では受信回路１３Ａの出力である受信された暗号化信号Ｂ′中の符号誤りを検出する誤り検出回路２８Ａが設けられている。またランダムパタン生成回路２１Ａ，２４Ａにより生成されたランダムパタンはパタンメモリ３８Ａ，３９Ａに取り込まれ、そこから変換回路２２Ａ及び逆変換回路２５Ａに与えられる。誤り検出回路２８Ａは例えばよく知られているＣＲＣ誤り検出方法を用いたものであり、受信暗号化信号Ｂ′中の符号誤りを検出すると検出信号Ｅａをパタンメモリ３８Ａのインヒビット端子INH に与えると共に送信回路１２Ａにも与える。パタンメモリ３８Ａは検出信号Ｅａによりランダムパタン生成回路２１Ａからのランダムパタンの取り込みが禁止され、従ってそれまで保持していたランダムパタンは更新されず、再び論理変換回路２２Ａに供給される。論理変換回路２２Ａはそのランダムパタンにより情報信号Ａを暗号化し、送信回路１２Ａはその暗号化情報信号Ａ′の先頭に誤り検出信号Ｅａを付加して伝送路１０Ｌに送出する。誤り検出回路２８Ａが誤り検出信号Ｅａ（１ビット）を出力している限りこの動作は繰り返され、誤り検出信号Ｅａが出力されなくなるとパタンメモリ３８Ａはランダムパタン生成回路２１Ａからのランダムパタンの取り込みを再開する。

【００２７】一方、相手通信装置１００Ｂが受信暗号化信号Ａ′中に符号誤りを検出した場合、上記と同様の動作を行い、その結果、暗号化情報信号Ｂ′に誤り検出信号Ｅｂが付加されて通信装置１００Ａに送信される。通信装置１００Ａの受信回路１３Ａは受信暗号化信号Ｂ′中に誤り検出信号Ｅｂが付加されているのを検出するとその信号Ｅｂにより逆変換部１８Ａのパタンメモリ３９Ａの取込み動作を禁止する。従ってそれまでパタンメモリ３９Ａに保持されていたランダムパタンを使って逆変換回路２５Ａにより受信暗号化信号Ｂ′の復号が行われる。このようにして受信信号Ｂ′中に符号誤りが検出された場合には、その誤りを含む受信情報信号Ｂにもとづいてランダムパタン生成回路２１Ａで発生されるランダムパタンを使用しないで、その直前に生成したランダムパタンを使って情報信号Ａの暗号化を行うと共に、相手通信装置１００Ｂに誤り検出信号Ｅａの送信するので、正しい復号化及び暗号化処理を継続することができる。なお、誤り検出信号Ｅａ，Ｅｂ自体の伝送路上での符号誤りの影響を回避するため、例えば誤り検出信号Ｅａ，Ｅｂを複数回送信し、受信側において多数決により、誤り信号を判別してもよい。

【００２８】上述した図５、図１０及び図１３の各実施例では情報信号Ａを暗号化するためのランダムパタンは復号化後の情報信号Ｂを使ってランダムパタン生成回路２１Ａにより生成し、また暗号化受信信号Ｂ′を復号するためのランダムパタンは暗号化前の情報信号Ａを使ってランダムパタン生成回路２４Ａにより生成する場合を示したが、逆に復号化前の受信信号Ｂ′を使って情報信号Ａを暗号化するためのランダムパタンを生成し、暗号化された情報信号Ａ′を使って受信信号Ｂ′を復号するためのランダムパタンを生成してもよい。その場合の暗号化通信装置１００Ａの例を図５と対応させて図１４に示す。その通信装置１００Ａの動作原理は図５の場合と同様なので説明を省略する。

【００２９】以上説明したこの発明の暗号化通信装置及び暗号化伝送システムは１対１の暗号化通信の場合であったが、この発明はそれに限定されるものでなく、１対複数（ポイントーマルチポイント）の伝送システムにも適用できることは明らかである。その例を図１５に示す。この伝送システムにおいては通信装置１００Ａは伝送路１０Ｌを通して複数、例えば２つの通信装置１００Ｂ，１００Ｃと多重通信を行う。多重化方法は時分割多重、周波数多重、あるいはその他の多重化方法を使ってよい。ここで通信装置１００Ａをセンタ装置と呼び、通信装置１００Ｂ，１００Ｃを加入者装置と呼ぶことにする。センタ装置１００Ａは加入者装置１００Ｂ，１００Ｃに対しそれぞれ送信すべき情報信号Ａ１，Ａ２を変換部１７Ａ１，１７Ａ２により加入者装置１００Ｂ，１００Ｃからの復号情報Ｂ，Ｃを使ってそれぞれ暗号化する。この時これまでの実施例の場合と同様に情報信号Ａ１，Ａ２は情報メモリ２３Ａ１，２３Ａ２にキー情報としてそれぞれ保持される。暗号化情報信号Ａ１′，Ａ２′は多重化回路５４で多重化され、送信回路１２Ａにより伝送路１０Ｌに送出される。

【００３０】加入者装置１００Ｂは受信回路１３Ｂにより受信したセンタ装置１００Ａからの多重化信号から分離回路５５Ｂにより自分宛の暗号化情報信号Ａ１′を分離し、逆変換部１８Ｂにおいて情報メモリ２３Ｂに保持してあるキー情報、即ち前回に送信した情報信号Ｂを使って復号して情報信号Ａ１を得る。加入者装置１００Ｂは更に次に送信する情報信号Ｂを情報メモリ３２Ｂに格納すると共にこの復号情報信号Ａ１を使って変換部１７Ｂにより暗号化し、その暗号化情報信号Ｂ′を送信回路１２Ｂにより伝送路１０Ｌに送出する。ただし、この伝送システムがＴＤＭＡのような同期形時分割多重方式を利用している場合は信号Ｂ′の送出は加入者装置１００Ｂに割当てられたタイムスロットを使って行われ、非同期形の時分割多重を利用している場合はアドレスが付加されたパケットを使って行われ、周波数多重を利用している場合は割当てられた周波数を使って行われる。加入者装置１００Ｃも同様の動作により復号情報信号Ａ２を得ると共に情報信号Ｃを送信する。センタ装置１００Ａは受信回路１３Ａにより受信した多重化信号を分離回路５５Ａにより分離して加入者装置１００Ｂ，１００Ｃからの暗号化情報信号Ｂ′，Ｃ′を得て、それらをそれぞれ逆変換部１８Ａ１，１８Ａ２によりそれぞれ情報メモリ２３Ａ１，２３Ａ２に保持してあるキー情報Ａ１，Ａ

２を使って復号し、情報信号Ｂ，Ｃを得る。

【００３１】図１５の暗号化伝送システムにおける各通信装置１００Ａ，１００Ｂ，１００Ｃの変換部１７Ａ１，１７Ａ２，１７Ｂ，１７Ｃ、逆変換部１８Ａ１，１８Ａ２，１８Ｂ，１８Ｃに前述した図６，８及び９やその他各種のランダムパタン生成回路を適用できることはいうまでもない。また各通信装置１００Ａ，１００Ｂ，１００Ｃにおいて図４に示すようにスクランブル回路１１Ａ、デスクランブル回路１４Ａ、擬似ランダムパタン発生器１５Ａ，１６Ａを設け、各装置の送信側においては送信情報信号を固定擬似ランダムパタンで暗号化してから変換部により受信信号にもとづいて暗号化し、受信側においては受信信号を逆変換部で復号してからデスクランブル回路１４Ａで固定擬似ランダムパタンにより最終的に復号するようにしてもよい。また図１０に示すようにパタン縮退回路２６Ａ，２７Ａにより情報信号をその複数の異なる部分パタンが同一の部分パタンとなるようにパタン変換してから、それにもとづいてランダムパタンを発生してもよい。更に図１３を参照して説明したように誤り検出回路２８Ａを設け、かつ変換部及び逆変換部のランダムパタン生成回路で生成されたランダムパタンをパタンメモリ３８Ａ，３９Ａに格納してから変換回路及び逆変換回路に与えるようにし、受信信号中に符号誤りを検出した場合はその検出信号を相手通信装置に送信すると共にパタンメモリへのランダムパタンの書き込みを禁止するよう構成してもよい。また図２及び図１５に示したこの発明の暗号化伝送システムでは伝送路１０Ｌは電気信号ケーブルに限定されず、電波の空間伝播路であってもよく、光ファイバ伝送路であってもよい。

【００３２】図１５のポイントーマルチポイント伝送システムに光ファイバ伝送方式を適用した場合の実施例を図１６に示す。センタ装置１００Ａからの共通の光ファイバ伝送路１０Ｌに複数の加入者装置１００Ｂ，１００Ｃからの個別光ファイバ線路Ｌａ，Ｌｂが方向性光分岐器５７によりそれぞれ接続されており、センタ装置１００Ａが送出する多重化信号は図１５の場合と同様に同報的にすべての加入者装置１００Ｂ，１００Ｃに送信される。図１５の場合と同様に各加入者装置においては自分以外の加入者装置に送信された信号を容易に分離して取り出すことができ、従ってセンタ装置１００Ａから各加入者装置１００Ｂ，１００Ｃへ送信される信号は暗号化されている必要がある。しかしながら各加入者装置は方向性光分岐器５７で光ファイバ伝送路１０Ｌに接続されているので、各加入者装置から送信される送信信号は他のいずれの加入者装置にも洩れることなく、センタ装置１００Ａにのみ送信することができる。従って図１６の実施例においては加入者装置１００Ｂ，１００Ｃから送出する信号は暗号化しないで送出している。センタ装置１００Ａは図１５における逆変換部１８Ａ１，１８Ａ２，情報メモリ２３Ａ１，２３Ａ２を有しておらず、光受信回路１３Ａで受信した多重化信号を分離回路５５Ａにより各加入者装置１００Ｂ，１００Ｃからの情報信号Ｂ，Ｃに分離し、その情報信号Ｂ，Ｃを使って変換部１７Ａ１，１７Ａ２において送信すべき情報信号Ａ１，Ａ２を暗号化する。暗号化情報信号Ａ１′，Ａ２′は多重化回路５４により多重化され、光送信回路１２Ａにより光カプラ５６Ａを通して光ファイバ伝送路１０Ｌに送出される。送信信号は方向性光分岐器５７により分岐され全ての加入者装置１００Ｂ，１００Ｃに供給される。各加入者装置１００Ｂ，１００Ｃは図１５における変換部１７Ｂ，１７Ｃを有しておらず、装置１００Ｂで代表して説明するように光受信回路１３Ｂにより受信した多重化信号から分離回路５５Ｂにより自分宛の暗号化信号Ａ１′を分離し、逆変換部１８Ｂにおいて情報メモリ２３Ｂに保持してあるキー情報、即ち前回の送信情報信号Ｂを使って受信暗号化信号Ａ１′を復号し、情報信号Ａ１を得る。加入者装置１００Ｂが送信すべき情報信号Ｂは暗号化せずそのまま光送信回路１２Ｂにより光カプラ５６Ｂ、及び方向性光分岐器５７を通して光ファイバ伝送路１０Ｌに送出される。

【００３３】図１６の実施例においても各変換部１７Ａ１，１７Ａ２と逆変換部１８Ｂ，１８Ｃを単純な排他的論理和回路で実現してよいし、更に秘話性を高めるため図５の場合のように各変換部１７Ａ１，１７Ａ２をランダムパタン生成回路２１Ａと論理変換回路２２Ａにより構成し、各逆変換部１８Ｂ，１８Ｃをランダムパタン生成回路２４Ａと論理逆変換回路２５Ａとにより構成してもよい。その場合、各ランダムパタン生成回路として前述したような各種の実施例を適用することができる。なお、センタ装置１００Ａは通常伝送システム全体を制御する機能を持たされており、また各加入者装置が図６または図８のランダムパタン生成回路に使用する生成多項式または識別番号ＩＤを全て持っている。

【００３４】更に図４の実施例のようにセンタ装置１００Ａにおいては変換部１７Ａ１，１７Ａ２の入力側とスクランブル回路を設けて送信すべき情報信号Ａ１，Ａ２をあらかじめ固定パタンで暗号化すると共に分離回路５５Ａにより分離された受信情報信号をデスクランブル回路により復号して情報信号Ｂ，Ｃを得るようにしてもよい。この場合、各加入者装置１００Ｂ，１００Ｃにおいても逆変換部１８Ｂ，１８Ｃの出力側にデスクランブル回路を設け、また送信情報信号の入力側にスクランブル回路を設け、送信すべき情報信号Ｂ，Ｃをあらかじめスクランブル回路により暗号化してから送信処理を行うように構成する。

【００３５】更に図１６の実施例に図１０で説明したパタン縮退回路２６Ａ，２７Ａの使用を適用してもよい。また図１３の実施例を図１６に適用することもできる。即ちセンタ装置１００Ａの各変換部１７Ａ１，１７Ａ２を図１３に示す変換部１７Ａと同じ構成とし、分離回路

５５Ａの各分離出力側に誤り検出回路をそれぞれ接続する。各誤り検出回路の誤り検出出力は対応する変換部のパタンメモリにインヒビット信号として与えると共に多重化回路５４に与え、暗号化情報信号Ａ１′Ａ２′の多重化の際に対応する暗号化情報信号の例えば先頭に誤り検出信号を表す符号（１ビット）を付加する。各加入者装置１００Ｂ，１００Ｃにおいては逆変換部１８Ｂ，１８Ｃを図１３の逆変換部１８Ａと同じ構成とし、分離回路５５Ｂ，５５Ｃの出力にそれぞれ誤り検出符号検出器を接続し、その検出出力を逆変換部１８Ｂ，１８Ｃのパタンメモリにインヒビット信号として与える。

【００３６】次に図１６の実施例においてセンタ装置１００Ａと加入者装置１００Ｂ，１００Ｃ間の信号の伝送方式を表すタイムチャートの例をいくつか示す。なお図が繁雑となるので暗号化後の情報信号は上述で使用したダッシュを付けないで暗号化前の情報信号と同じ記号で表す。また、破線矢印Ｅｎは暗号化処理を表し、破線矢印Ｄｅは復号処理を表す。

【００３７】図１７は加入者装置１００Ｂ，１００Ｃからセンタ装置１００Ａへの上り信号とその逆の下り信号をＴＤＭＡのように送受信のタイミングが同期した時分割多重する場合のタイムチャートを示し、信号送受信周期（即ち繰返し周期）T_f が一定の場合である。センタ装置１００Ａから加入者装置１００Ｂ，１００Ｃ宛の暗号化信号$A1_1$，$A2_1$（一定長）があらかじめそれぞれの加入者装置に割り当てられたタイムスロットで送信され、加入者装置１００Ｂ，１００Ｃはそれぞれ自分に割り当てられたタイムスロットから暗号化信号$A1_1$，$A2_1$ を抽出し、前回の送信情報（図示せず）を使って復号し、一定時間T_X 後に情報信号B_1，C_1 を送出する。センタ装置１００Ａは情報信号B_1，C_1 を受信し、その情報信号を使って次に送信する情報$A1_2$，$A2_2$ を暗号化し、前回の送信から時間T_f 後に所定のタイムスロットで送信する。加入者装置１００Ｂ，１００Ｃはそれぞれ受信した暗号化情報$A1_2$，$A2_2$ をそれぞれ前回の送信情報信号B_1，C_1 を使って復号し、一定時間T_X後に情報信号B_2，C_2 をそれぞれ送信する。以下同様の動作が繰り返えされる。

【００３８】図１８は送受信のタイミングが非同期で時分割多重を行う方式の信号送受タイムチャートを示す。センタ装置１００Ａは各加入者装置から受けた最新の復号受信情報を少なくとも次の復号受信信号が得られるまで保持する機能を有しており、各加入者装置１００Ｂ，１００Ｃに対しそれらのアドレスが先頭に付加された暗号化情報信号をパケットとして任意のタイミングで送信する。各加入者装置１００Ｂ，１００Ｃは送信すべき情報信号Ｂ，Ｃの先頭に自分のアドレスを付加したパケットを任意のタイミングで送信する。ただし、センタ装置１００Ａも、加入者装置１００Ｂ，１００Ｃもすべて信号衝突検出機能を有し、信号送出中に信号衝突を検出した場合はそのパケットの送信をやりなおす。

【００３９】図１９は上り信号と下り信号を別々の光ファイバ線路、または異なる波長で伝送する場合の伝送方式の一例を示すタイムチャートである。この伝送方式の例においては、センタ装置１００Ａは各加入者装置宛の送信信号$A1_1$，$A2_2$，…，$A2_1$，$A2_2$，…をあらかじめ各加入者装置に割り当てたタイムスロットに時分割多重して連続して送信すると同時に、加入者装置１００Ｂ，１００Ｃからの送信信号B_1，B_2，…及びC_1，C_2，…も時分割多重されて連続して受信することができる特徴がある。

【００４０】図１７～１９のいずれの伝送方式においても、センタ装置１００Ａと各加入者装置１００Ｂ，１００Ｃ間の通信において上り信号と下り信号の伝送容量が不平衡の場合は、例えば変換部において送信情報信号を暗号化するのに使用する受信情報信号はその一部を使用するか、あるいは一連の送信情報信号に対し同一の受信情報信号を複数回使用するようにすればよい。

【００４１】以上説明したように、この発明による暗号化通信装置によれば、復号受信信号または受信暗号化信号を使って変換部により送信すべき情報信号を暗号化して送出すると共に、送信情報信号または暗号化情報信号をキー情報として情報メモリに相手装置からの応答情報信号の受信時まで記憶しておき、情報メモリから読み出された前回の情報信号送信時のキー情報を使って逆変換部において暗号化受信信号を復号するように構成されている。暗号化及び復号化に使用する情報は随時変化するので秘話性の高い通信が可能な暗号化通信装置を実現することができる。更に、伝送路を通して少なくとも２つの通信装置が接続されたこの発明の暗号化伝送システムによれば、第１の通信装置においては受信信号を使って送信すべき情報信号を変換部において暗号化して第２の通信装置へ送出し、第２通信装置においては情報メモリに保持されている前回の情報信号であるキー情報を使って逆変換部により復号するように構成されている。暗号化に使用する受信信号は随時変化していくので秘話性の高い暗号化伝送システムを実現することができる。

【図面の簡単な説明】

【図１】従来の暗号化伝送システムの一例を示すブロック図。

【図２】この発明による暗号化伝送システムの一実施例を示すブロック図。

【図３】図２の動作例を説明するための各信号の変化を示す表。

【図４】この発明の伝送システムにおける暗号化通信装置の一実施例を示すブロック図。

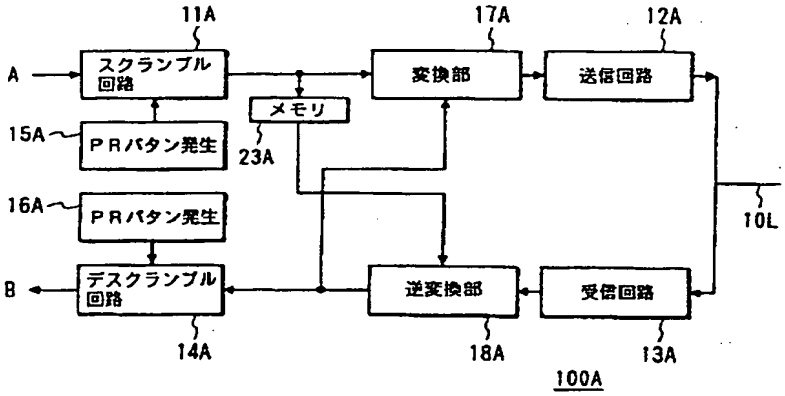
【図５】暗号化通信装置の他の実施例を示すブロック図。

【図６】ランダムパタン生成回路の一実施例を示すブロック図。

【図７】図６における非線形演算回路の実施例を示すブロック図。
【図８】ランダムパタン生成回路の他の実施例を示すブロック図。
【図９】ランダムパタン生成回路の他の実施例を示すブロック図。
【図１０】暗号化通信装置の更に他の実施例を示すブロック図。
【図１１】図１０におけるパタン縮退回路の実施例を示すブロック図。
【図１２】図１０のパタン縮退回路の入出力関係を示す表。
【図１３】暗号化通信装置の更に他の実施例を示すブロック図。
【図１４】暗号化通信装置の更に他の実施例を示すブロック図。
【図１５】暗号化伝送システムの他の実施例を示すブロック図。
【図１６】暗号化伝送システムの更に他の実施例を示すブロック図。
【図１７】この発明の暗号化伝送システムにおける同期形時分割多重による交信例を示すタイムチャート。
【図１８】この発明の暗号化伝送システムにおける非同期形時分割多重による交信例を示すタイムチャート。
【図１９】上り信号と下り信号に別々の伝送線路を設けたこの発明の暗号化伝送システムにおける交信例を示すタイムチャート。

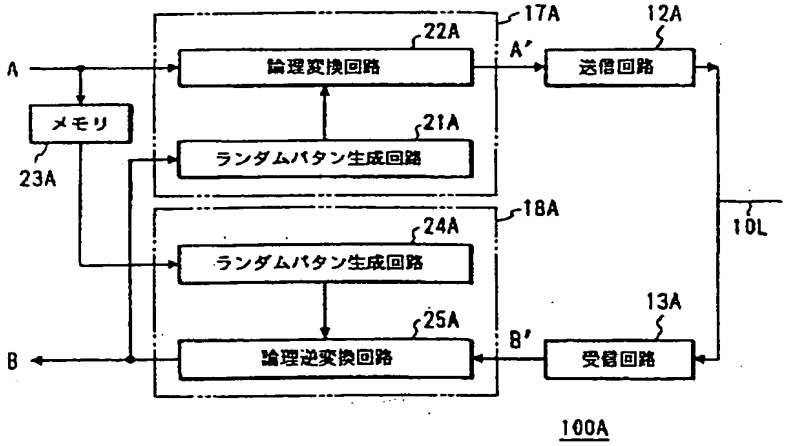
【図４】

図４



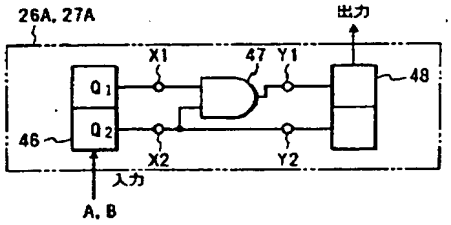
【図５】

図５



【図１１】

図１１



【図１２】

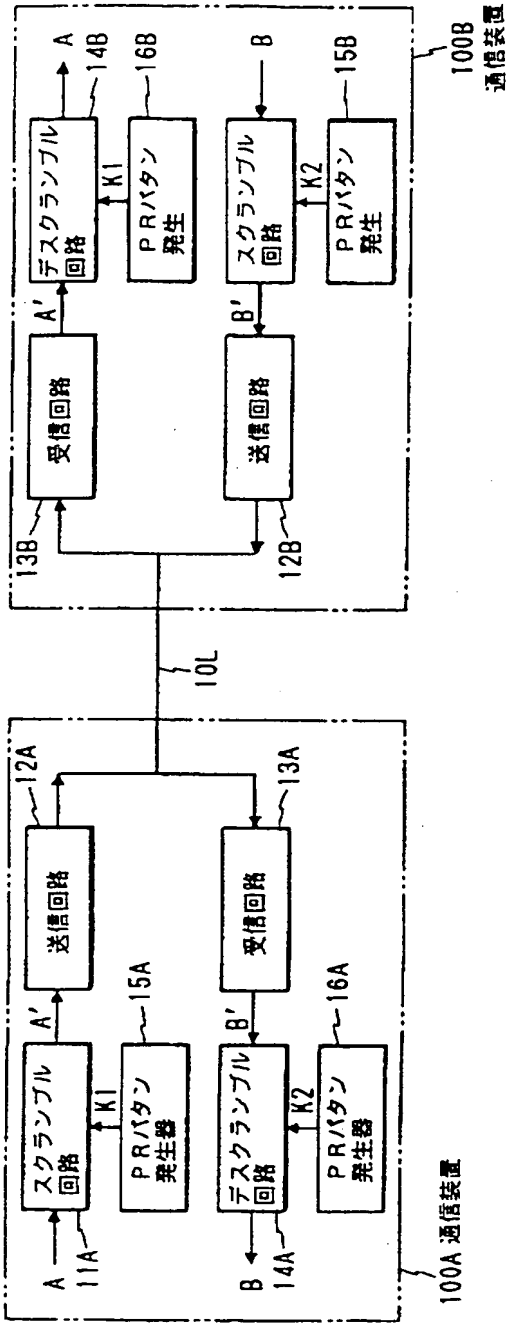
図１２

表II

入力		出力	
X1	X2	Y1	Y2
0	0	0	0
0	1	0	1
1	0	0	0
1	1	1	1

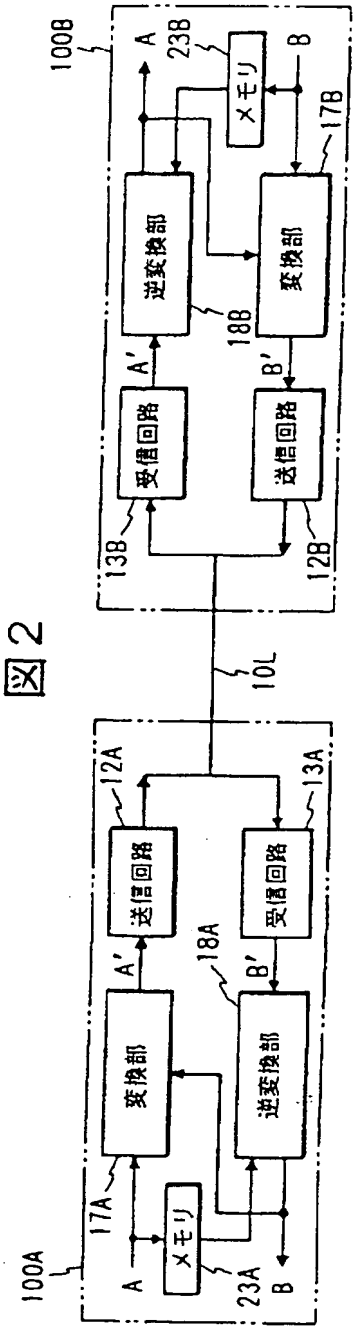
【図1】

図1


100B 通信装置
A
14B
16B
B
15B
デスクランブル回路
K1
PRパタン発生
スクランブル回路
K2
PRパタン発生
A'
B'
受信回路
送信回路
13B
12B
10L
12A
13A
送信回路
受信回路
A'
B'
スクランブル回路
K1
PRパタン発生器
デスクランブル回路
K2
PRパタン発生器
15A
16A
A
11A
B
14A
100A 通信装置

【図2】

図2


100B
A
23B
メモリ
B
17B
逆変換部
変換部
18B
A'
B'
受信回路
送信回路
13B
12B
10L
12A
13A
送信回路
受信回路
A'
B'
18A
変換部
逆変換部
17A
メモリ
A
23A
B
100A

【図３】

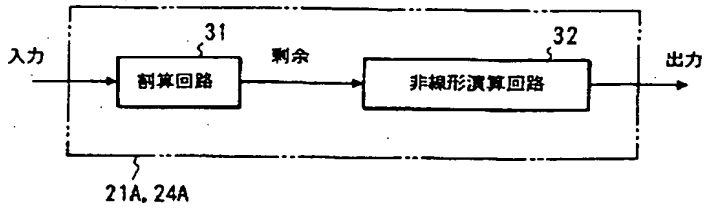
図３

表１

通信装置 100A		通信装置 100B
B_0 : 0 0 0 0 0 0 0 0		B_0 : 0 0 0 0 0 0 0 0
A_1 : 1 0 1 0 1 0 1 0		A_1' : 1 0 1 0 1 0 1 0
$A_1 \oplus B_0 = A_1'$: 1 0 1 0 1 0 1 0	$A_1' \oplus B_0 = A_1$	B_1 : 0 0 0 0 1 1 1 1
B_1' : 1 0 1 0 0 1 0 1		$A_1 \oplus B_1 = B_1'$: 1 0 0 1 0 0 1 1
$A_1 \oplus B_1' = B_1$: 0 0 0 0 1 1 1 1	$A_1 \oplus B_1 = B_1'$	A_2' : 0 0 1 1 0 0 1 1
A_2 : 0 0 1 1 0 0 1 1		$A_2' \oplus B_1 = A_2$: 0 0 1 1 0 0 1 1
$A_2 \oplus B_1 = A_2'$: 0 0 1 1 1 1 0 0	$A_2' \oplus B_1 = A_2$	B_2 : 1 1 1 1 0 0 0 0
B_2' : 1 1 0 1 0 0 0 1		$A_2 \oplus B_2 = B_2'$: 1 1 0 1 0 0 0 1
$A_2 \oplus B_2' = B_2$: 1 1 1 0 0 0 1 0	$A_2 \oplus B_2 = B_2'$	

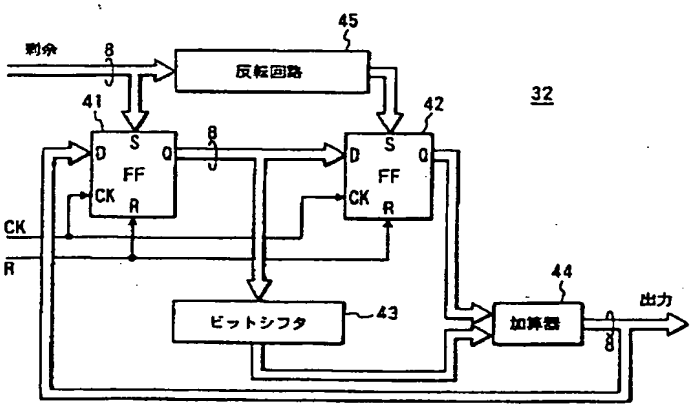
【図６】

図６



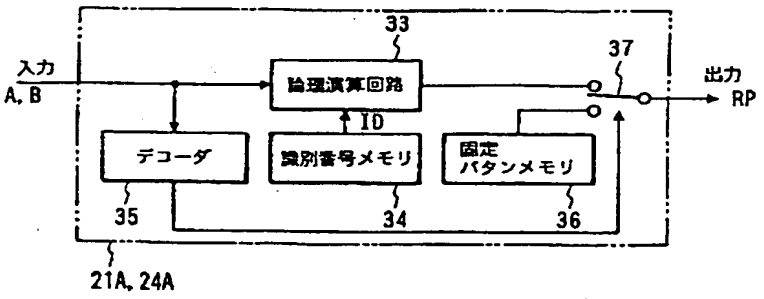
【図７】

図７



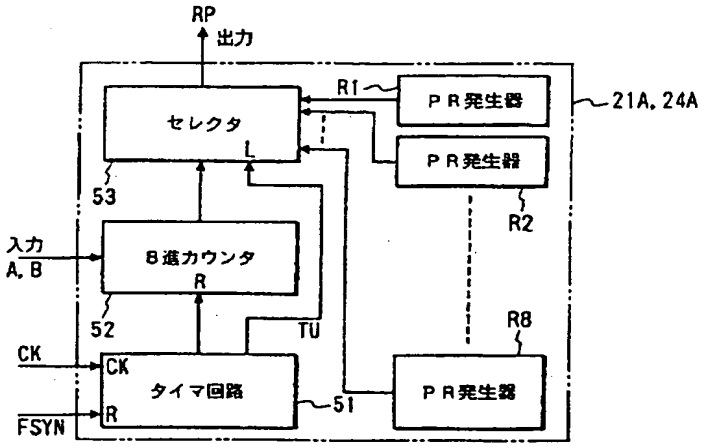
【図８】

図８



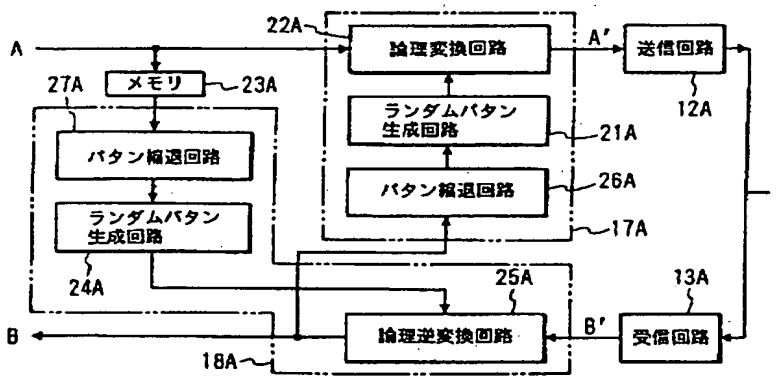
【図９】

図９



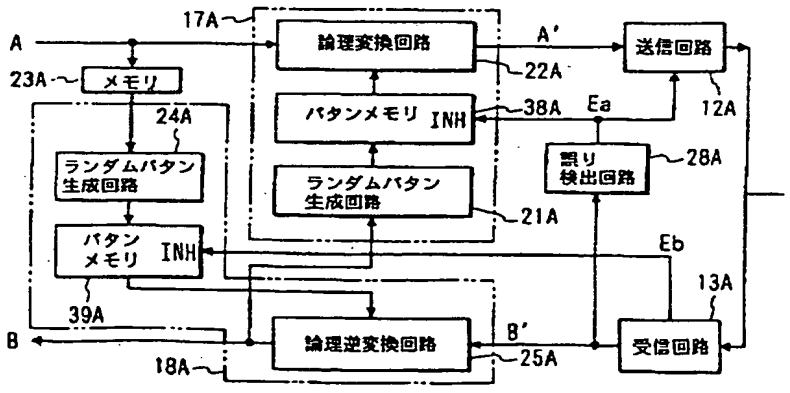
【図１０】

図１０



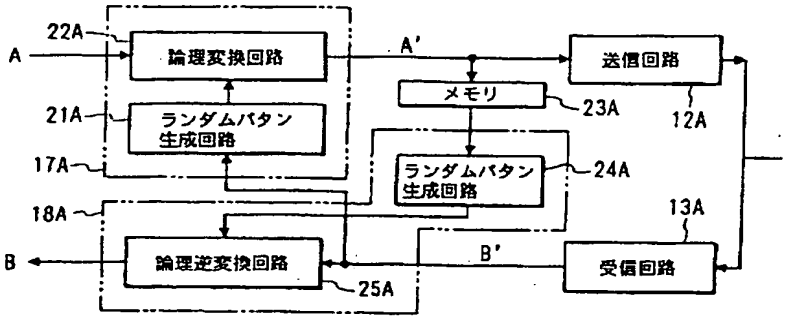
【図１３】

図１３



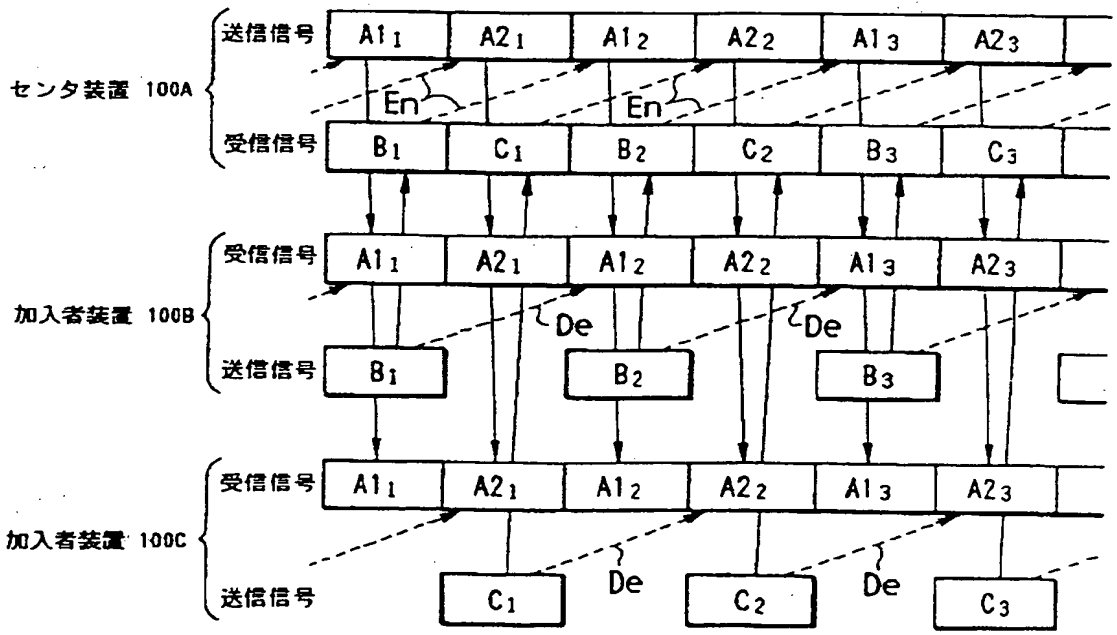
【図１４】

図１４



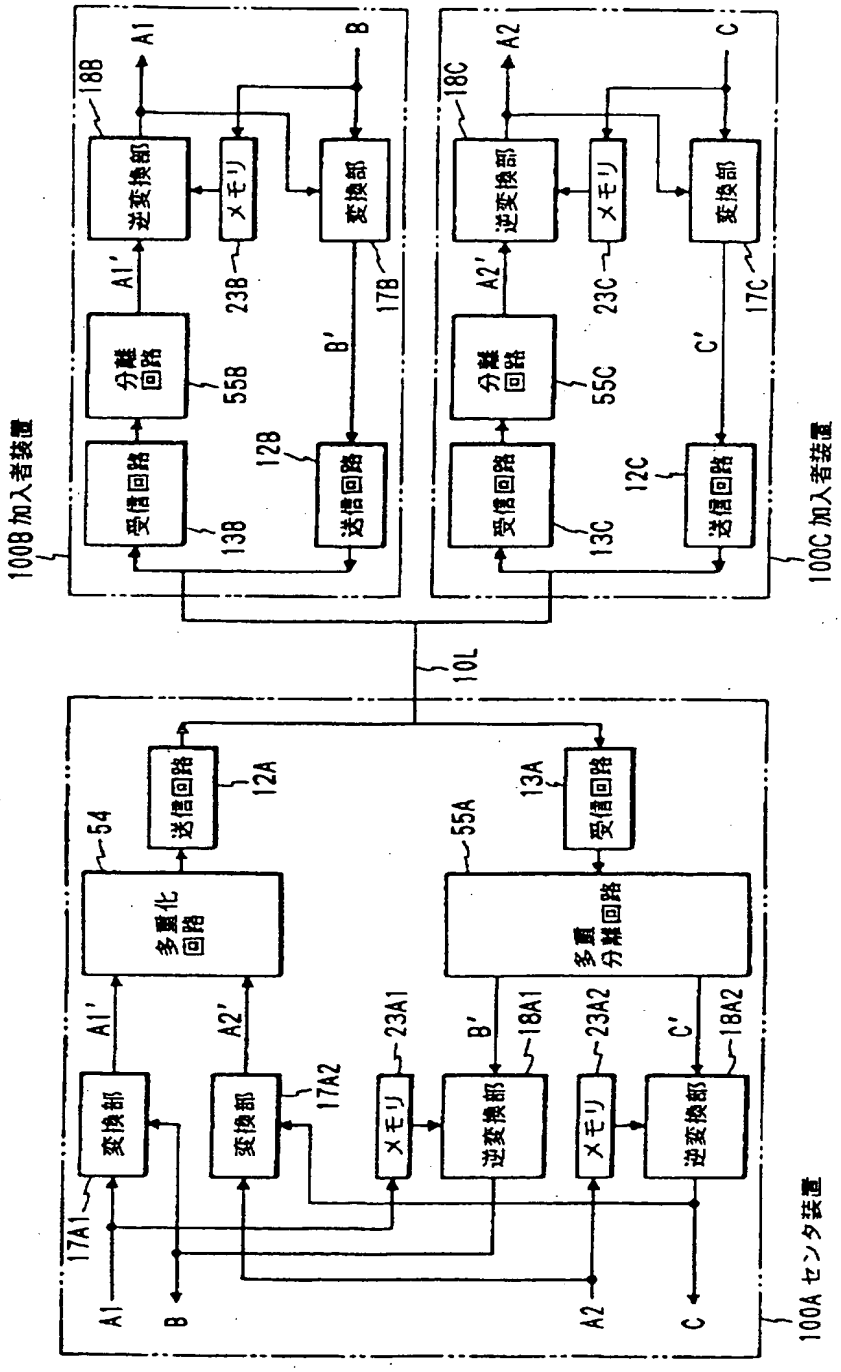
【図１９】

図１９



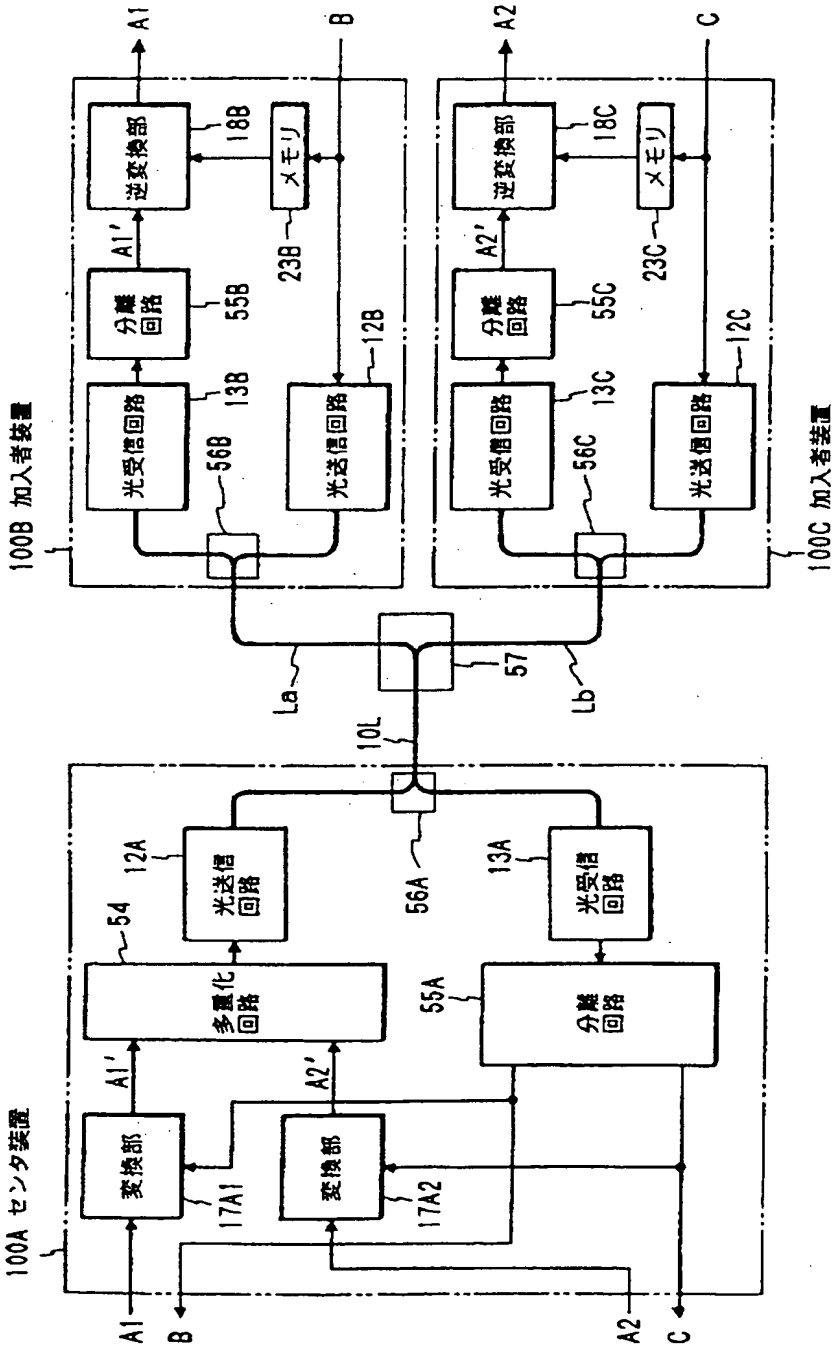
【図１５】

図１５


100A センタ装置
100B 加入者装置
100C 加入者装置
10L
多重化回路
多重分離回路
送信回路
受信回路
変換部
逆変換部
メモリ
分離回路
A1
A2
B
C
A1'
A2'
B'
C'
12A
13A
12B
13B
12C
13C
17A1
17A2
17B
17C
18A1
18A2
18B
18C
23A1
23A2
23B
23C
54
55A
55B
55C

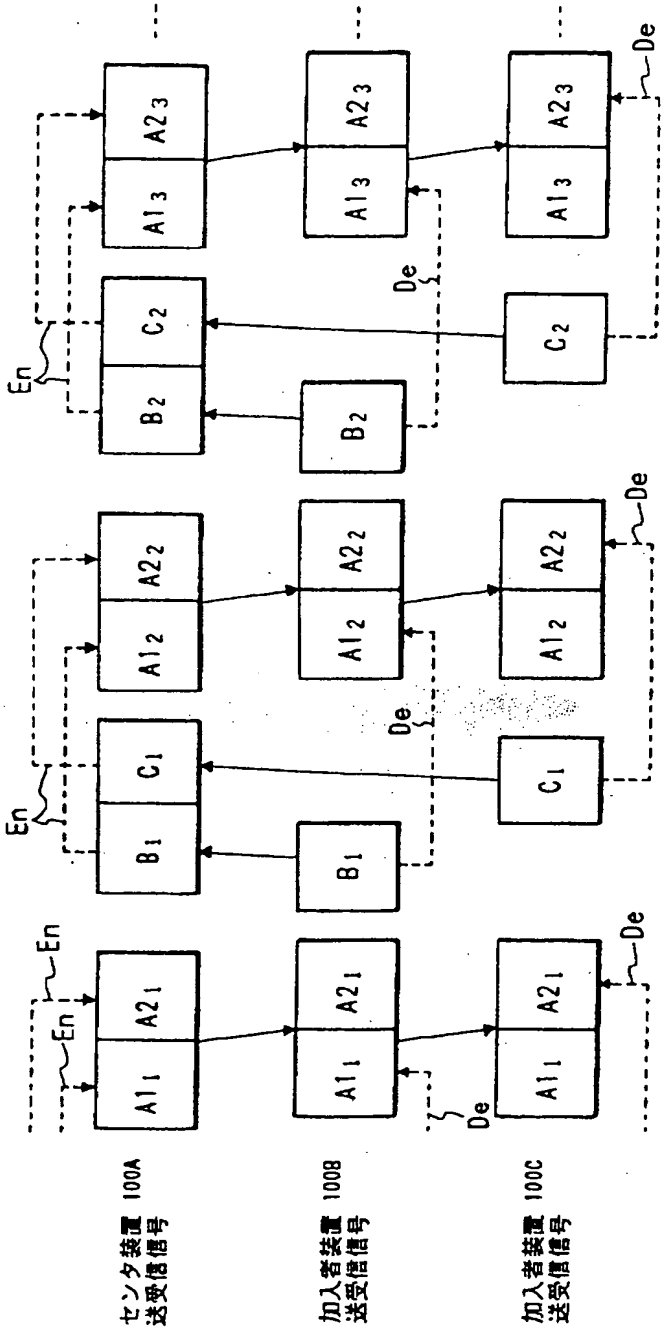
【図１６】

図１６


100A センタ装置
100B 加入者装置
100C 加入者装置
A1
B
A2
C
変換部
17A1
17A2
多重化回路
54
光送信回路
12A
光受信回路
13A
分離回路
55A
56A
10L
La
57
Lb
光受信回路
13B
光送信回路
12B
分離回路
55B
逆変換部
18B
メモリ
23B
光受信回路
13C
光送信回路
12C
分離回路
55C
逆変換部
18C
メモリ
23C
56B
56C
A1'
A2'

【図１７】

図１７


センタ装置 100A 送受信信号
加入者装置 100B 送受信信号
加入者装置 100C 送受信信号
En
De
A1 1
A2 1
B1
C1
A1 2
A2 2
B2
C2
A1 3
A2 3

【図１８】

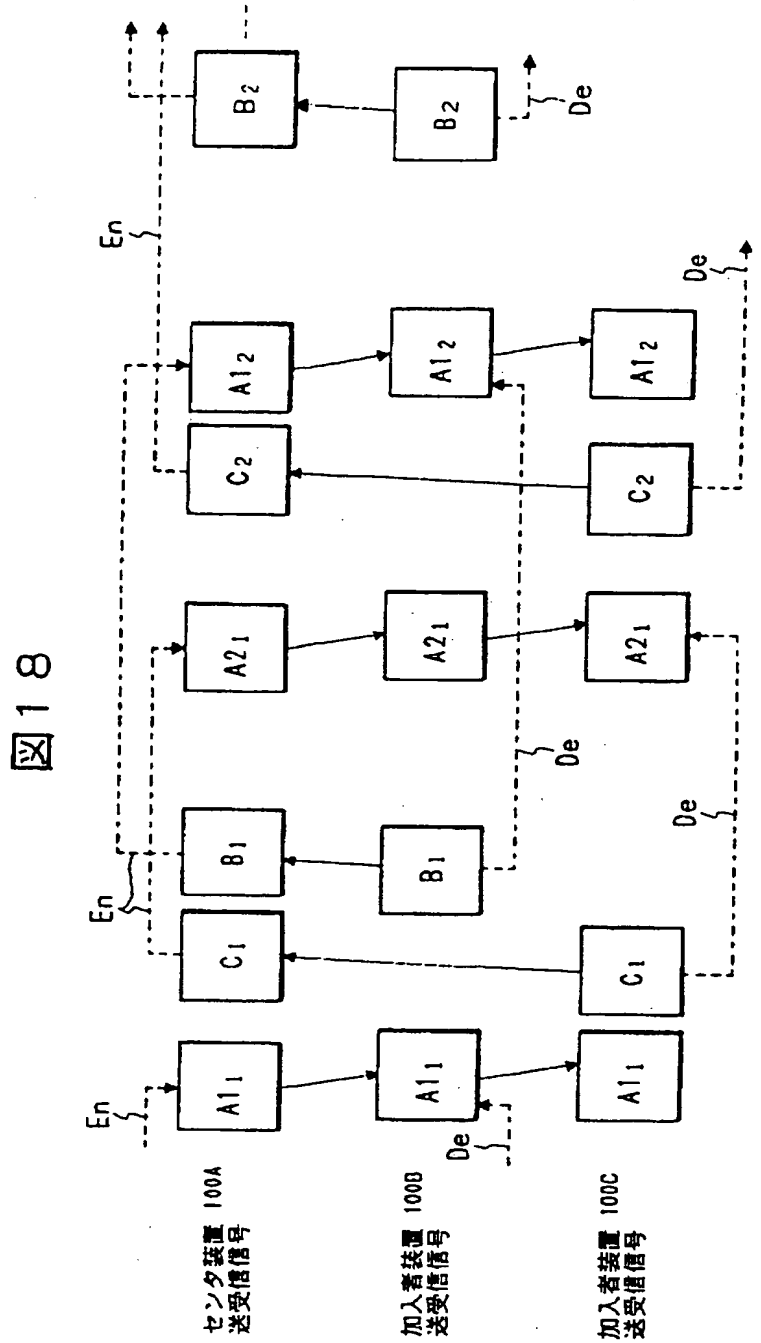


図１８

フロントページの続き

(72)発明者　雲崎　清美
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　三鬼　準基
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内